Cybersecurity Tips

The following provides some of the ways you can protect yourself and your organization from cyber threats, but is not intended to be an exhaustive list. If you suspect you have been the target of a cyber threat, contact your FSO or security point of contact.

Employees

- Use complex alphanumeric passwords
- Change passwords regularly
- Do NOT open an email or attachment from an unfamiliar source, even if it looks official
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department
- Report all suspicious or unusual problems with your computer to your IT department

Management and IT Departments

- Implement defense-in-depth; a layered defense strategy that includes technical, organizational, and operational controls
- Implement technical defenses, including firewalls, intrusion detection systems, and Internet content filtering
- Update anti-virus software daily
- Regularly download vendor security patches for all software
- Change the manufacturer's default passwords on all software
- Monitor, log, and analyze successful and attempted intrusions to your systems and networks